# Technology Safety Plan Tip Sheet for Survivors

## Prioritize Safety

### Consider using a safer device.

- If you think that someone is monitoring your computer, tablet, or smartphone:
    - Try using a different device that the abusive partner hasn't had physical or remote access to (like a computer at a library or a friend's phone).

- This is one way to reduce the risk of being monitored by an abusive partner.

### Get more information.

- Navigating violence, abuse, and stalking can be very difficult and dangerous. Anti-violence workers in your area can tell you about options and local resources and help you create a plan for your safety.
- You can call your local anti-violence organization to be connected with a support worker near you or find one at www.sheltersafe.ca.

### Trust your instincts.

- Abusive partners are often very determined to maintain control over survivors and technology is one of many tools they use to do this.
- If it seems like the person knows too much about you, they could be getting information from a variety of sources, like:
    - monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.

### Strategically plan around your tech.

- When abusers misuse technology, it's often a natural reaction to want to throw away devices or close online accounts to make it stop.
- However, some abusive individuals may escalate their controlling and dangerous behaviour if they feel they've lost control over their current or former partner.
- Before removing a hidden camera or GPS tracker that you've found, or uninstalling stalkerware, think through how your former partner may respond and plan for your safety.

- For example: Some survivors choose to use a safer device for certain interactions but also keep using the monitored device as a way to collect evidence and prevent escalation.

## Identify the Abuse

### Look for patterns.

- Take time to think through what kind of technology may be used to stalk, monitor, or harass you.
  - For example, if the abuser has hinted that they are watching you, think about what they know.
- Do they only know what you are doing in a certain area of your home?
  - If so, there may be a hidden camera in that room.
- If you suspect you're being followed, is it just when you're in your car, or is it also when you are on foot?
  - If it's just in your car, then there may be a device hidden in your car.
  - If it's everywhere, it may be something you are carrying with you, such as your phone or a tracker in your bag.
- Narrowing down the potential source of technology being misused can help you create a safety plan and to document the abuse.
- Read more about Assessing for Technology-Facilitated Violence.

### Document the incidents.

- Documenting a series of incidents can show police or the court a pattern of behaviour that fits a legal definition of stalking or harassment.

- Documentation can also help you see if things are escalating and help you with safety planning.
- For more information, check out Documentation Tips for Women Experiencing Technology-Facilitated Violence.

### Report the incidents.

- You may also want to report the incidents to law enforcement or seek a Peace Bond or Family Protection Order.
- If the harassing behaviour is online, you can also report the abuse to the website or app where the harassment is happening.
- If the behaviour violates the platform's terms of service, the content may be removed or the person may be banned.
- It's important to recognize that reporting content may remove it completely, so it should be documented as evidence before reporting it.

## Steps to Increase Security

### Change passwords and usernames.

- If you think your online accounts are being accessed, you can change your usernames and passwords using a safer device.
- Once you've updated the account information, it's important not to access those accounts from a device you think is being monitored.
- Consider creating brand new accounts, such as a new email address with a non-identifying username instead of your actual name or other revealing information.
- It's important not to link these new accounts to any old accounts or numbers, and not to use the same password for all of your accounts.

- Read more tips about Password Safety.

## Check your devices and settings.

- Go through your smartphone, apps, and online accounts to check the privacy settings to make sure that other devices or accounts aren't connected to yours and that any device-to-device access, like Bluetooth, is turned off when you're not using it.
- Make sure you know what each of your apps are and what it does.
- Delete any apps on your device that you're unfamiliar with or that you don't use.
- Look for spikes in data usage – these may indicate that monitoring software such as spyware is in use.

## Get a new device.

- If you suspect that your actual device is being monitored, the safest thing may be to get a new device with an account that your current/former partner doesn't have access to.
- A pay-as-you-go phone is a less expensive option.
- Put a passcode on the new device and don't link it to your old cloud accounts like iCloud or Google that the person might have access to.
- Consider turning off location and Bluetooth sharing when it's not in use.
- You also might keep the old device so that the perpetrator thinks you are still using it and doesn't try to get access to the new device.

## Protect your location.

- If the abuser seems to always know where you are, they might be tracking you through your smartphone or vehicle or by using a location-tracking device.
- You can check your smartphone, apps, and accounts to see if location sharing is turned on and update the settings to best suit your needs.
- You can also call your wireless provider to ask if any location-sharing services are in use, especially if you were/are on a family plan with the your current/former partner.
- Location tracking through your car might be through a roadside assistance or safe driver service.
- If you are concerned about a hidden tracking device in your car or other belongings, law enforcement or a car mechanic may be able to check for you.
- It's important to safety plan and document evidence before removing a device or changing the abuser's access to your location information.

## Consider cameras and audio devices.

- If you suspect that you're being monitored through cameras or audio recorders, it may be happening through hidden devices, gifts received from your current/former partner, or even everyday devices like webcams, personal assistants (such as Google Home or Alexa), or security systems.
- If you're concerned about hidden cameras, you may consider trying a camera detector, though some will locate only wireless cameras, not wired cameras, or vice versa.
- Everyday devices or gifts may be able to be secured by changing account settings or passwords.

- Built-in web cameras can be covered with a piece of removable tape (although this only addresses the camera, not the spyware on the computer).
- Remember to make a safety plan and document evidence before removing devices or cutting off the abuser's access.

## Steps to Increase Privacy

### Protect your address.

- If you're concerned about someone discovering your home address, you could open a private mailbox (PO Box).
- Note that this is most helpful if you have recently moved or your current/former partner doesn't already know your address.
- Tell friends and family not to share your address and be cautious about giving it out to local businesses.
- Also, look into what information is public in your community if you were to purchase a home so you know your options.

### Limit the information you give out about yourself.

- Almost everything we do these days asks for personally identifying information – whether it's to make a purchase, open a discount card, or create an online account.
- The information we provide is often sold to third parties.
- When possible, opt out of information collection, or only provide the minimum amount necessary.
- You can get creative – for instance, instead of using your first and last name, use your first and last initials.

- You can also use a free virtual phone number, such as Google Voice, to give yourself an alternative number to share when you need to.

## Control your offline and online privacy.

- Our Technology Safety and Privacy Toolkit has Online Privacy and Safety Tips, including more information about changing settings on your electronic devices, social media accounts such as Facebook and X, and your home Wi-Fi network.
- Follow those steps to increase your privacy and decrease the risks of the abuser misusing those technologies, locating you, or monitoring your activity.

*Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.*

*Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource Technology Safety Plan: A Guide for Survivors and Advocates.*